

#2  
12/14/01  
PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

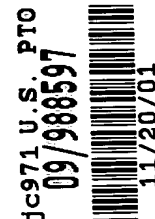
In re application of

Katsuya SHINOHARA

Serial No. (unknown)

Filed herewith

CHAINING KEY BROADCASTING RECEPTION SYSTEM AND  
CHAINING KEY BROADCASTING RECEPTION METHOD



**CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119**  
**AND SUBMISSION OF PRIORITY DOCUMENT**

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan under 2000-355123, filed on 22 November 2000.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel  
Benoît Castel  
Attorney for Applicant  
Customer No. 000466  
Registration No. 35,041  
745 South 23rd Street  
Arlington, VA 22202  
703/521-2297

November 20, 2001

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

Jc971 U.S. PTO

09/988597



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出 願 年 月 日

Date of Application:

2000年11月22日

出 願 番 号

Application Number:

特願2000-355123

出 願 人

Applicant(s):

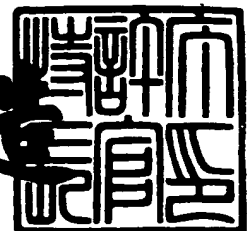
日本電気株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 8月31日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 68501895

【提出日】 平成12年11月22日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

    【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

    【氏名】 篠原 克也

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

    【識別番号】 100088812

    【弁理士】

    【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

    【予納台帳番号】 030982

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9001833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 連鎖鍵放送受信システム及び連鎖鍵放送受信方法

【特許請求の範囲】

【請求項 1】 デジタル放送を受信するための連鎖鍵放送受信システムであって、前記デジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得る手段を有することを特徴とする連鎖鍵放送受信システム。

【請求項 2】 前記鍵情報を得る手段は、前記コンテンツを復号化するための連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子とを受信する連鎖鍵受信手段と、前記対象鍵識別子を用いて既に保存されている連鎖鍵を取出す連鎖鍵保存手段と、前記連鎖鍵保存手段から送られてくる連鎖鍵を用いて前記連鎖鍵受信手段が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する連鎖鍵復号化手段とを含むことを特徴とする請求項 1 記載の連鎖鍵放送受信システム。

【請求項 3】 前記連鎖鍵の受信と復号化と保存との一連の処理と、その連鎖鍵を用いる処理とを独立して実行するよう構成したことを特徴とする請求項 2 記載の連鎖鍵放送受信システム。

【請求項 4】 前記連鎖鍵を用いる処理が暗号化コンテンツの復号化処理であることを特徴とする請求項 3 記載の連鎖鍵放送受信システム。

【請求項 5】 任意の連鎖鍵の識別子を前記対象識別子として指定するようにしたことを特徴とする請求項 1 から請求項 4 のいずれか記載の連鎖鍵放送受信システム。

【請求項 6】 デジタル放送を受信するための連鎖鍵放送受信方法であって、前記デジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得るステップを有することを特徴とする連鎖鍵放送受信方法。

【請求項 7】 前記鍵情報を得るステップは、前記コンテンツを復号化するための連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子と

を受信するステップと、前記対象鍵識別子を用いて既に保存されている連鎖鍵を  
 取出すステップと、その取出された連鎖鍵を用いて受信した連鎖鍵を復号化して  
 新たな連鎖鍵を生成するステップとを含むことを特徴とする請求項 6 記載の連鎖  
 鍵放送受信方法。

【請求項 8】 前記連鎖鍵の受信と復号化と保存との一連の処理と、その連  
 鎖鍵を用いる処理とを独立して実行するようにしたことを特徴とする請求項 7 記  
 載の連鎖鍵放送受信方法。

【請求項 9】 前記連鎖鍵を用いる処理が暗号化コンテンツの復号化処理で  
 あることを特徴とする請求項 8 記載の連鎖鍵放送受信方法。

【請求項 10】 任意の連鎖鍵の識別子を前記対象識別子として指定するよ  
 うにしたことを特徴とする請求項 6 から請求項 9 のいずれか記載の連鎖鍵放送受  
 信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は連鎖鍵放送受信システム及び連鎖鍵放送受信方法に関し、特に暗号鍵  
 を用いてデスクランブルされるデジタル放送におけるスクランブル放送の受信  
 方法に関する。

【0002】

【従来の技術】

従来、鍵放送システムとしては、デジタル放送におけるスクランブル放送を  
 デスクランブルするための暗号鍵を受信して復号するために、CAS (C o n d  
 i t i o n a l A c c e s s S y s t e m : 限定受信) カードを用いるもの  
 がある。

【0003】

このCASカードの処理は、図 6 に示すように、作業鍵復号化モジュール 2 3  
 が番組に先立って放送されてくる暗号化されている作業鍵をCASカード内のマ  
 スタ鍵 2 4 を用いて復号化して作業鍵記憶部 2 1 に格納する。

【0004】

スクランブル鍵復号化モジュール 2 2 は番組と同時に放送されてくる暗号化されているスクランブル鍵を当該作業鍵記憶部 2 1 に格納された作業鍵を用いて復号化してカード外に出力する。尚、図示していないが、C A S カードの外ではスクランブルされている番組映像をスクランブル鍵を用いて復号化して表示している。

## 【 0 0 0 5 】

## 【発明が解決しようとする課題】

上述した従来の鍵放送システムでは、一つの番組の中でスクランブル鍵の復号化のために毎回同じ作業鍵を用いているため、予め作業鍵を入手しておけば、番組放送時には途中から視聴しても、また途中で視聴を一時中断しても、スクランブル鍵を生成することができるので、番組の最初から最後まで視聴した視聴者だけが鍵を使えるようにするといったサービスを実施することができないという問題がある。

## 【 0 0 0 6 】

また、暗号化されているスクランブル鍵を受信すると、復号化したスクランブル鍵を出力してしまうため、暗号化されているスクランブル鍵の受信と復号化したスクランブル鍵の利用とを非同期に行うことができないという問題がある。

## 【 0 0 0 7 】

さらにまた、作業鍵の保管とスクランブル鍵の出力とが全く別処理であるため、復号化したスクランブル鍵を次回以降のスクランブル鍵の復号化に用いる作業鍵として用いることができないという問題がある。

## 【 0 0 0 8 】

そこで、本発明の目的は上記の問題点を解消し、復号化した鍵を次回以降の復号に用いる処理を実現することができる連鎖鍵放送システム及び連鎖鍵放送方法を提供することにある。

## 【 0 0 0 9 】

## 【課題を解決するための手段】

本発明による連鎖鍵放送システムは、デジタル放送を受信するための連鎖鍵放送受信システムであって、前記デジタル放送における複数の番組を視聴した

時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得る手段を備えている。

#### 【0010】

本発明による連鎖鍵放送方法は、デジタル放送を受信するための連鎖鍵放送受信方法であって、前記デジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得るステップを備えている。

#### 【0011】

すなわち、本発明の連鎖鍵放送システムは、放送を受信する装置において複数の番組を視聴することによって、暗号化コンテンツを解く鍵を得ることができるようにしたことにある。

#### 【0012】

より具体的に、本発明の連鎖鍵放送システムは、連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子とを受信する連鎖鍵受信手段と、対象鍵識別子を用いて既に保存されている連鎖鍵を取出す連鎖鍵保存手段と、連鎖鍵保存手段から送られてくる連鎖鍵を用いて連鎖鍵受信手段が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する連鎖鍵復号化手段とを有している。

#### 【0013】

上記のような構成を採用することによって、一連の連鎖鍵を全て受信しないと最終的な連鎖鍵の復号化ができないという仕組みを実現することが可能となり、放送事業者が自番組を最初から最後まで視聴した、または自放送局の連続番組を欠かさず視聴した視聴者だけが最終的な連鎖鍵を入手することができるようなサービスを実施することが可能となる。例えば、番組Aと番組Bとを視聴した人が連鎖鍵Bを、番組Aと番組Cとを視聴した人が連鎖鍵Cをそれぞれ得られるというサービスが実現可能となる。

#### 【0014】

#### 【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。図1は本発明の実施の形態による連鎖鍵放送システムの構成を示すブロック図である。図1にお

いて、本発明の実施の形態による連鎖鍵放送システムは連鎖鍵受信手段 1 と、連鎖鍵復号化手段 2 と、連鎖鍵保存手段 3 とから構成されている。

## 【 0 0 1 5 】

連鎖鍵受信手段 1 は連鎖鍵、その鍵識別子、及びその鍵が復号化する連鎖鍵を示す対象鍵識別子を受信する。連鎖鍵保存手段 3 は連鎖鍵受信手段 1 で受信した対象鍵識別子を用いて既に保存されている連鎖鍵を取出す。連鎖鍵復号化手段 2 は連鎖鍵保存手段 3 から送られてくる連鎖鍵を用いて、連鎖鍵受信手段 1 が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する。

## 【 0 0 1 6 】

これによって、一連の連鎖鍵を全て受信しないと最終的な連鎖鍵の復号化ができないという仕組みを実現することができ、放送事業者が自番組を最初から最後まで視聴した、または自放送局の連続番組を欠かさず視聴した視聴者だけが最終的な連鎖鍵を入手することができるようなサービスを実施することができる。

## 【 0 0 1 7 】

図 2 は本発明の一実施例による連鎖鍵放送システムの構成を示すブロック図である。図 2 において、本発明の一実施例による連鎖鍵放送システムはデマックス 1 1 と、映像デコーダ 1 2 と、映像モニタ 1 3 と、連鎖鍵ハンドラ 1 4 と、連鎖鍵復号化モジュール 1 5 と、連鎖鍵管理モジュール 1 6 と、コンテンツ復号化モジュール 1 7 と、連鎖鍵メモリ 1 8 と、ハードディスク 1 9 とから構成されている。

## 【 0 0 1 8 】

デマックス 1 1 はデジタル放送信号を受信し、そのデジタル放送信号を動画・音声といった MPEG (Moving Picture Experts Group) データと、暗号化連鎖鍵と、鍵識別子と、対象鍵識別子とに分離する。

## 【 0 0 1 9 】

映像デコーダ 1 2 は MPEG データをデコードして映像データを生成する。映像モニタ 1 3 は映像デコーダ 1 2 が生成した映像データをモニタ (図示せず) に表示・再生する。



## 【 0 0 2 0 】

連鎖鍵管理モジュール 1 6 は連鎖鍵ハンドラ 1 4 から鍵識別子と暗号化連鎖鍵とを受取ると、暗号化連鎖鍵を連鎖鍵として識別子と対にして連鎖鍵メモリ 1 8 に記録し、連鎖鍵ハンドラ 1 4 から対象鍵識別子を受取ると、連鎖鍵メモリ 1 8 内で対象鍵識別子と対になっている連鎖鍵を連鎖鍵復号化モジュール 1 5 に送出する。

## 【 0 0 2 1 】

また、連鎖鍵管理モジュール 1 6 は連鎖鍵復号化モジュール 1 5 から鍵識別子と連鎖鍵とを受取ると、それらを対にして連鎖鍵メモリに記録し、コンテンツ復号化モジュール 1 7 から鍵識別子を受取ると、連鎖鍵メモリ 1 8 内で鍵識別子と対になっている連鎖鍵をコンテンツ復号化モジュール 1 7 に戻す。

## 【 0 0 2 2 】

連鎖鍵ハンドラ 1 4 はデマックス 1 1 から暗号化連鎖鍵と鍵識別子と対象鍵識別子とを受取る。連鎖鍵ハンドラ 1 4 は対象鍵識別子がヌルの場合、暗号化連鎖鍵が一連の最初の連鎖鍵であるとして、鍵識別子とともに連鎖鍵管理モジュール 1 6 に送出する。また、連鎖鍵ハンドラ 1 4 は対象鍵識別子がヌルではない場合、2 番目以降の暗号化連鎖鍵であるとして、対象鍵識別子を連鎖鍵管理モジュール 1 6 に送出し、暗号化連鎖鍵と鍵識別子とを連鎖鍵復号化モジュール 1 5 に送出する。

## 【 0 0 2 3 】

連鎖鍵復号化モジュール 1 5 は連鎖鍵管理モジュール 1 6 から受取った連鎖鍵を用いて、暗号化連鎖鍵を復号化し、新たな連鎖鍵を得て、鍵識別子とともに連鎖鍵管理モジュール 1 6 に送出する。

## 【 0 0 2 4 】

コンテンツ復号化モジュール 1 7 は連鎖鍵管理モジュール 1 6 に鍵識別子を送出し、連鎖鍵管理モジュール 1 6 から得た連鎖鍵を用いてハードディスク 1 9 内の暗号化コンテンツを復号化して目的のコンテンツ（復号化コンテンツ）を得る。ハードディスク 1 9 には予め放送や通信、配布媒体等を経由して入手した暗号化コンテンツが保存されている。

## 【 0 0 2 5 】

図 3 は図 2 の連鎖鍵メモリ 1 8 の構成を示す図である。図 3 において、連鎖鍵メモリ 1 8 には鍵識別子 #  $n$  ( $n = 1, 2, 3, 4, 5, \dots$ ) と、鍵識別子 #  $n$  と対の連鎖鍵 #  $n$  とが格納されている。

## 【 0 0 2 6 】

図 4 は本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理を示すフローチャートである。これら図 2 ～図 4 を参照して本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理について説明する。本発明の一実施例による連鎖鍵放送システムでは連鎖鍵ハンドラ 1 4 と連鎖鍵管理モジュール 1 6 と連鎖鍵復号化モジュール 1 6 とによって連鎖鍵が順次生成される。

## 【 0 0 2 7 】

暗号化連鎖鍵、その鍵識別子、及び対象鍵識別子が連鎖鍵ハンドラ 1 4 に与えられると（図 4 ステップ S 1）、連鎖鍵ハンドラ 1 4 は対象鍵識別子を判定し、対象鍵識別子がヌルであれば（図 4 ステップ S 2）、鍵識別子と暗号化連鎖鍵とを連鎖鍵管理モジュール 1 6 に送付し、連鎖鍵管理モジュール 1 6 がこれらに対して連鎖鍵メモリ 1 8 に格納する（図 4 ステップ S 7）。

## 【 0 0 2 8 】

連鎖鍵ハンドラ 1 4 は対象鍵識別子がヌルでなければ（図 4 ステップ S 2）、次のように暗号化連鎖鍵から新たな連鎖鍵を得て、連鎖鍵管理モジュール 1 6 がそれらを連鎖鍵メモリ 1 8 に格納する（図 4 ステップ S 6）。

## 【 0 0 2 9 】

暗号化連鎖鍵から新たな連鎖鍵を得る手順は、まず連鎖鍵ハンドラ 1 4 が対象鍵識別子を連鎖鍵管理モジュール 1 6 に送り、連鎖鍵管理モジュール 1 6 がその対の連鎖鍵を連鎖鍵復号化モジュール 1 5 に送出する（図 4 ステップ S 3）。同時に、連鎖鍵ハンドラ 1 4 は鍵識別子と暗号化連鎖鍵とを連鎖鍵復号化モジュール 1 5 に送出する（図 4 ステップ S 4）。

## 【 0 0 3 0 】

連鎖鍵復号化モジュール 1 5 は連鎖鍵ハンドラ 1 4 が得た暗号化連鎖鍵を、連鎖鍵管理モジュール 1 6 から得た連鎖鍵で復号化し、新たな連鎖鍵を得る（図 4

ステップ S 5)。連鎖鍵復号化モジュール 1 5 は新たな連鎖鍵と連鎖鍵管理モジュール 1 6 から得た鍵識別子とを連鎖鍵管理モジュール 1 6 に送出し、連鎖鍵管理モジュール 1 6 はこれらに対して連鎖鍵メモリ 1 8 に格納する（図 4 ステップ S 6）。

#### 【0031】

図 5 は本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理を示すフローチャートである。これら図 2 と図 3 と図 5 とを参照して本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理について説明する。本発明の一実施例による連鎖鍵放送システムではコンテンツ復号化モジュール 1 7 及び連鎖鍵管理モジュール 1 6 によって、連鎖鍵を用いて暗号化コンテンツを復号化している。

#### 【0032】

この場合、コンテンツ復号化モジュール 1 7 は鍵識別子を指定して連鎖鍵管理モジュール 1 6 から連鎖鍵を取出す（図 5 ステップ S 1 1）。コンテンツ復号化モジュール 1 7 は連鎖鍵管理モジュール 1 6 から得た連鎖鍵を用いて暗号化コンテンツを復号化する（図 5 ステップ S 1 2）。

#### 【0033】

このように、前回に受信した鍵で次に受信した鍵を順次復号化することによって、番組を最初から最後まで視聴したり、連続ドラマを全回視聴したりして一連の鍵を全て受信した視聴者だけが最終的な鍵を得ることができる。例えば、所望のコンテンツを復号化して入手できるような放送サービスを実現することができる。

#### 【0034】

また、連鎖鍵の受信・復号化・保存の一連の処理と、その連鎖鍵を用いる処理、例えば暗号化コンテンツの復号化処理とを独立して実施させることによって、連鎖鍵の受信・復号化・保存を行っていない時（例えば、番組を視聴していない時）でも、鍵を用いて蓄積媒体等に保存された暗号化コンテンツを復号化することができる。

#### 【0035】

さらに、任意の連鎖鍵の識別子を対象識別子として指定することによって、必ずしも連鎖鍵を順番に放送する必要はなく、例えば番組Aで連鎖鍵Aを放送し、番組Bで送る連鎖鍵Bの対象鍵識別子を連鎖鍵A、番組Cで送る連鎖鍵Cの対象鍵識別子も同じく連鎖鍵Aとすることで、番組Aと番組Bとを視聴した人は連鎖鍵Bを、番組Aと番組Cとを視聴した人は連鎖鍵Cを得ることができるといったサービスを柔軟に実施することができる。したがって、復号化した鍵を次回以降の復号に用いる処理を実現することができる。

#### 【0036】

#### 【発明の効果】

以上説明したように本発明によれば、デジタル放送を受信するための連鎖鍵放送受信システムにおいて、デジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得ることによって、復号化した鍵を次回以降の復号に用いる処理を実現することができるという効果がある。

#### 【図面の簡単な説明】

#### 【図1】

本発明の実施の形態による連鎖鍵放送システムの構成を示すブロック図である。

#### 【図2】

本発明の一実施例による連鎖鍵放送システムの構成を示すブロック図である。

#### 【図3】

図2の連鎖鍵メモリの構成を示す図である。

#### 【図4】

本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理を示すフローチャートである。

#### 【図5】

本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理を示すフローチャートである。

#### 【図6】

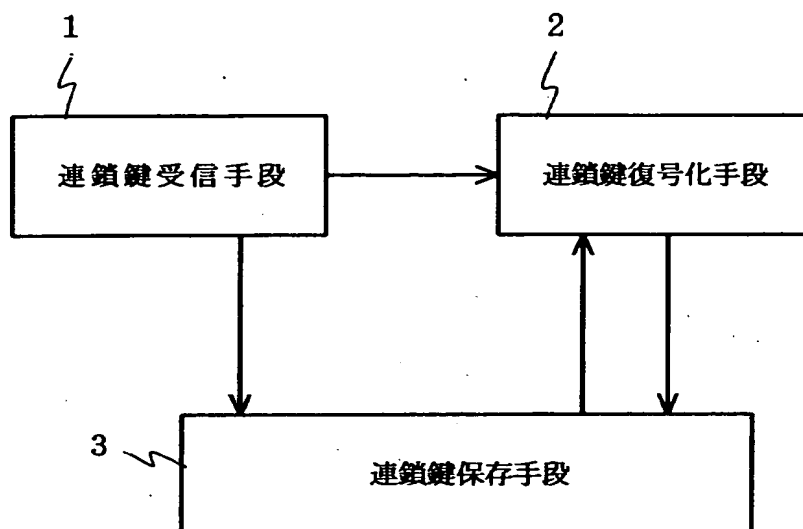
従来例による鍵放送システムの構成を示すブロック図である。

【符号の説明】

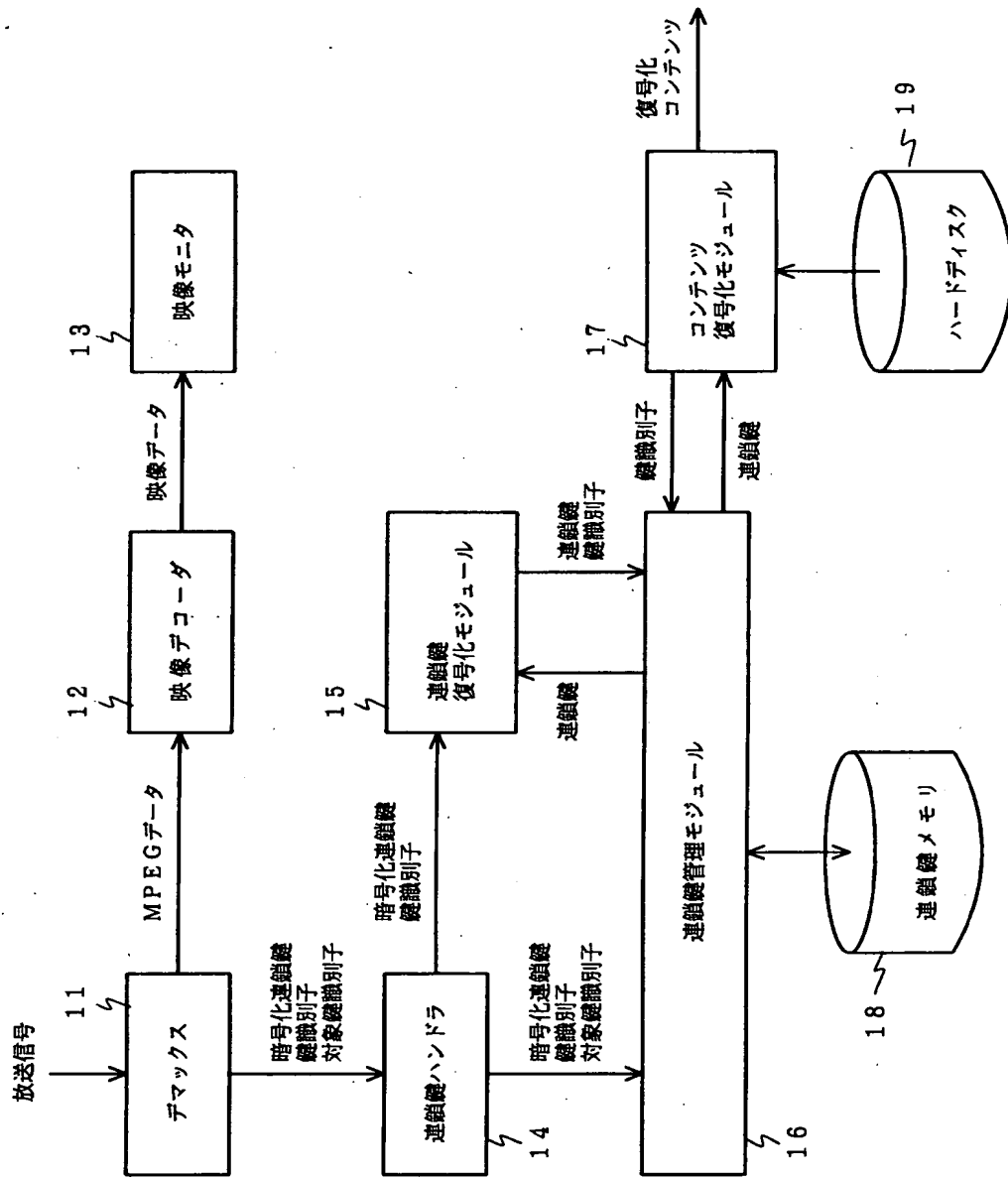
- 1 連鎖鍵受信手段
- 2 連鎖鍵復号化手段
- 3 連鎖鍵保存手段
- 1 1 デマックス
- 1 2 映像デコーダ
- 1 3 映像モニタ
- 1 4 連鎖鍵ハンドラ
- 1 5 連鎖鍵復号化モジュール
- 1 6 連鎖鍵管理モジュール
- 1 7 コンテンツ復号化モジュール
- 1 8 連鎖鍵メモリ
- 1 9 ハードディスク

【書類名】 図面

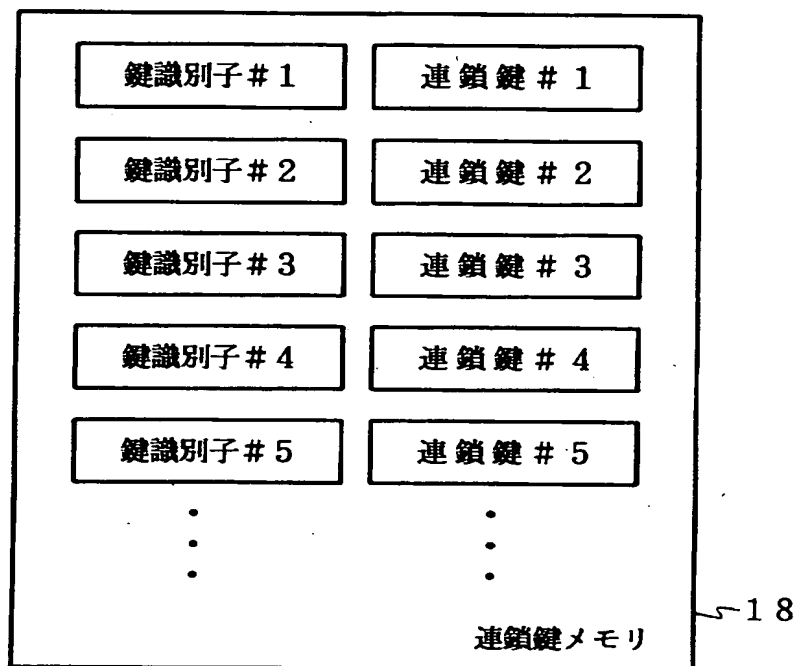
【図 1】



【図 2】

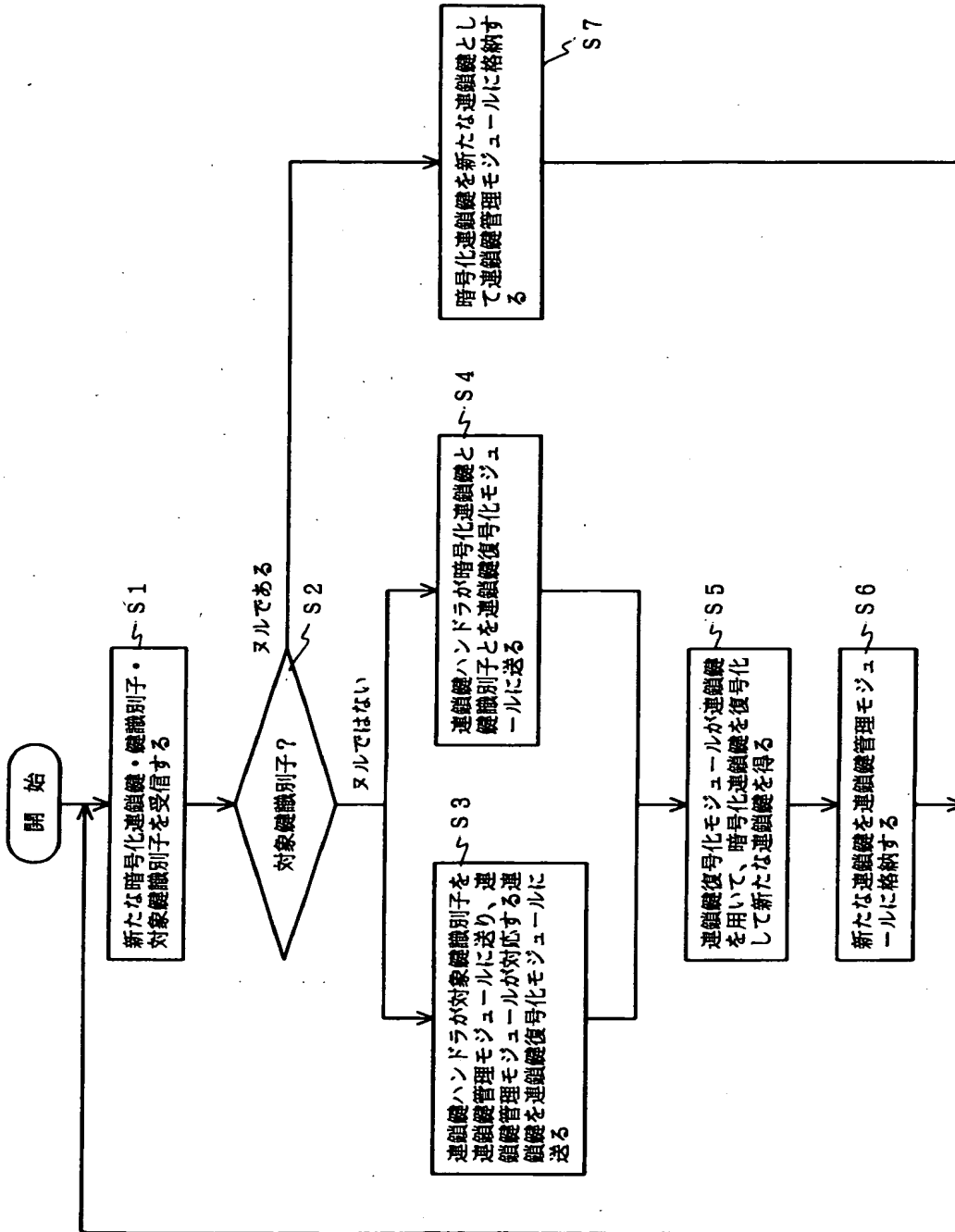


【図 3】

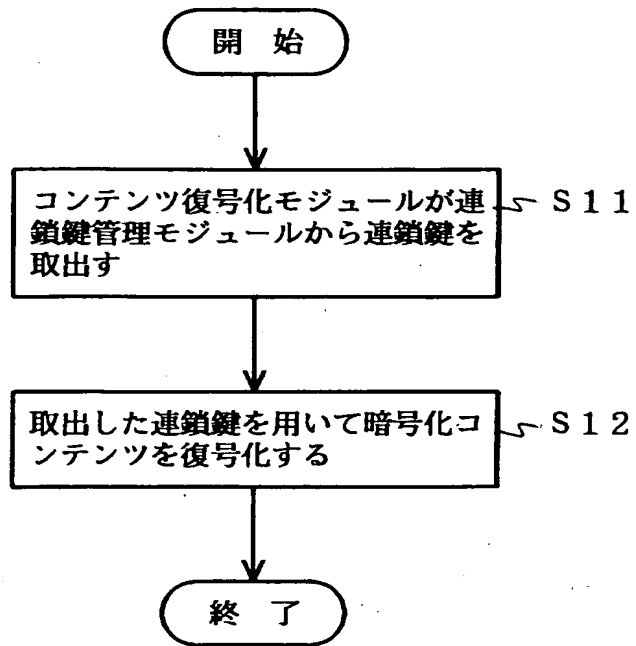




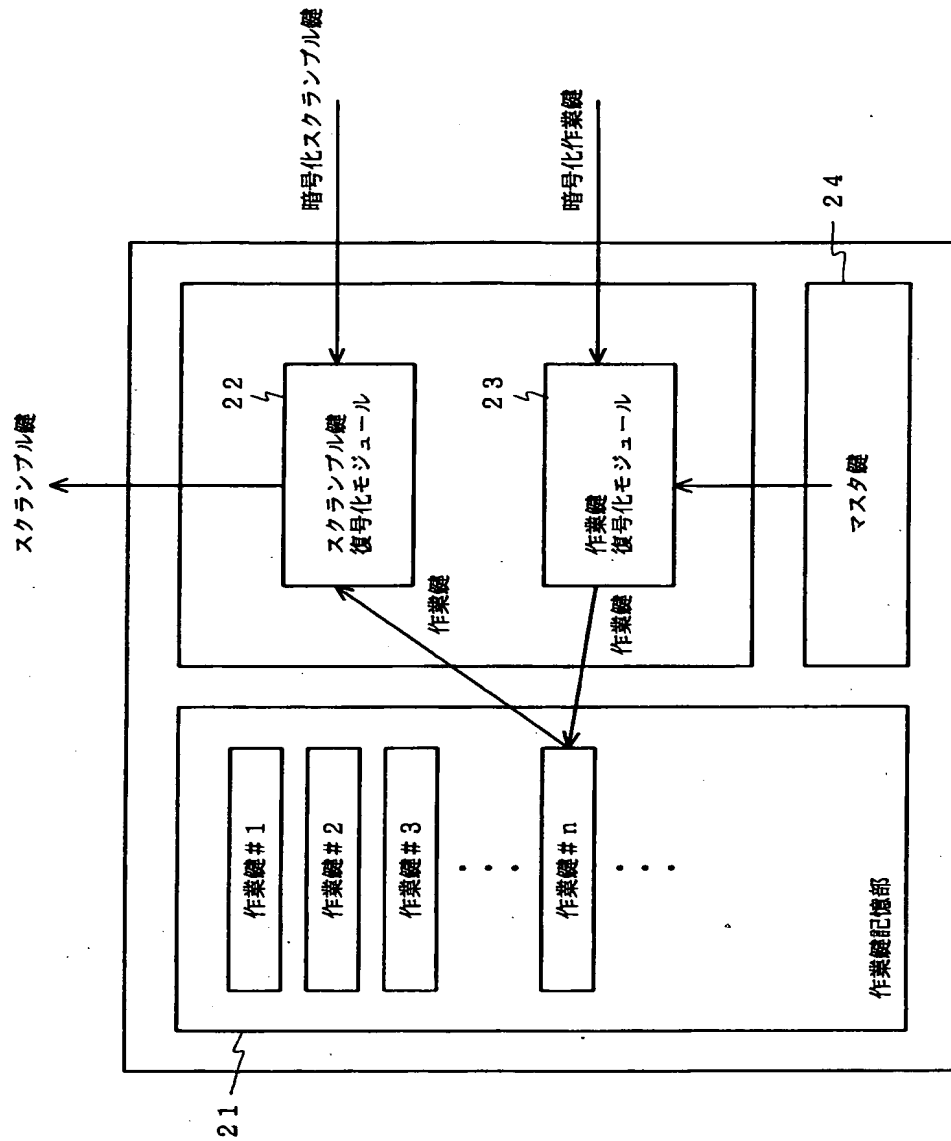
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 復号化した鍵を次回以降の復号に用いる処理が実現可能な連鎖鍵放送システムを提供する。

【解決手段】 連鎖鍵受信手段 1 は連鎖鍵、その鍵識別子、及びその鍵が復号化する連鎖鍵を示す対象鍵識別子を受信する。連鎖鍵保存手段 3 は連鎖鍵受信手段 1 で受信した対象鍵識別子を用いて既に保存されている連鎖鍵を取出す。連鎖鍵復号化手段 2 は連鎖鍵保存手段 3 から送られてくる連鎖鍵を用いて、連鎖鍵受信手段 1 が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社